Security and Anonymity in the Digital Age- A Nationalist Perspective

Everyone is aware we live in a digital age, and if we are to make use of this to assist in our aims, then we at least need to know who to use the tools we are wielding.

Some people scoff at these beliefs, thinking there is no need to learn anything regarding computer security-either because it is too difficult, or because it is simply paranoid fantasy. This attitude is largely due to media influence, which often stylises hackers and likes to show the System as being ahead of all digital trends and able to lock you away for life simply by logging where you last put a usb stick. The reality is that the hackers are always 10 steps ahead of the security agencies working in hand with the police and government organisations.

The recent scandals exposed by Edward Snowden have shown our governments can and DO spy on its citizens. If the government is so eager to spy on the average joe, how much interest do you think they have in dedicated Nationalists?

Whether you choose to take on board the measures I present here or not, the advice I offer is relevant to all who are currently scrutinised by those in power as ‘subversive elements of society’.

I’ll begin with discussing the basics. I hope to show that anyone can apply these measures, and they require minimal amount of computer knowledge and tech know how.

For those more interested in learning how to implement these measures to a more thorough degree, further info will be available. Anyone who says you cannot be anonymous on the internet is either a fool or a shill.

Computers and the subsequent interaction between systems is complex. And it doesn't help that so called beginner's guides are written by experienced experts who write from a point of view where they take much of their knowledge for granted and thus end up alienating the reader.

This isn’t a guide on hacking btw; this will be a focus on security at all levels when using computer systems.

Getting started

The best place to begin is the basic entry units; that is, what you're using to access the internet. This is hardware-your computer or laptop, and software such as the *operating system* (OS) (either Windows, Mac or Linux). Your first line of defence is installing a firewall, and it is assumed everyone has one of these on their computer. Securing the basics and learning all about such basics is a great way to begin.

How I started was by speaking with hackers, reading their forums and generally lurking about the internet, seeing what basic stuff I could teach myself. I knew that 90% of individuals get caught because:

1.they use Windows

2. they don't anonymise and encrypt their traffic (they don't use an IP masking *proxy*- or better yet a *VPN*). By traffic, I mean the flow of information from the internet to their computer and vice versa. The best way to do that is with a little tool called Tor.

The Tor Network

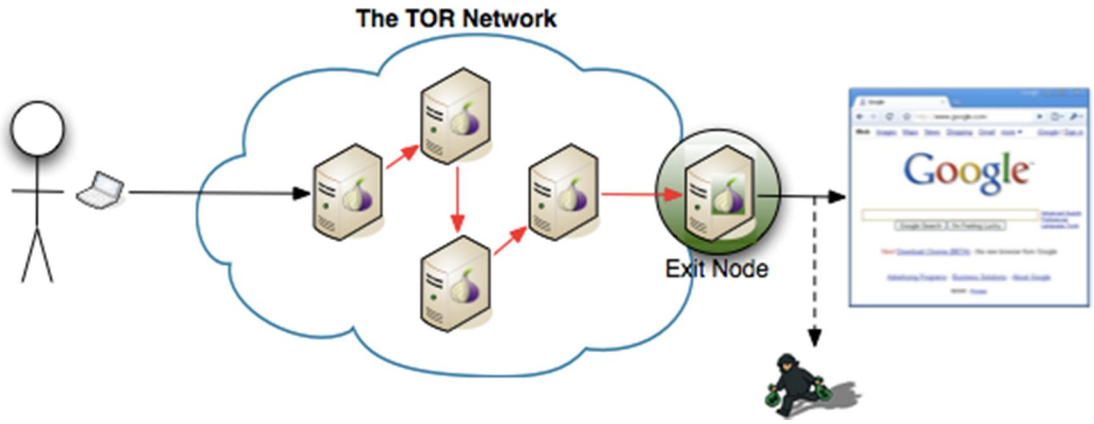
www.torproject.org

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

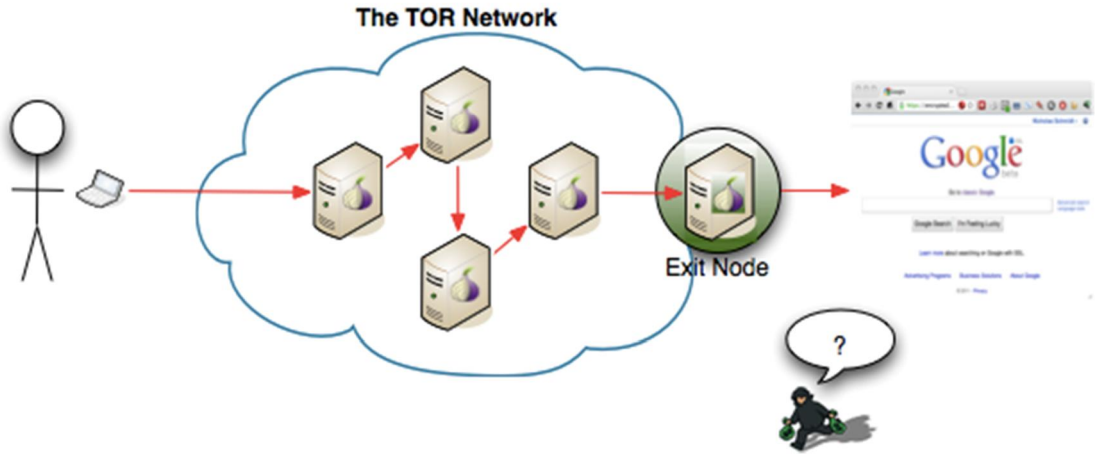
Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Tor operates in the same manner as a VPN. It essentially changes your IP and is a trusted and constantly updated project, which has been used as an essential tool by Wikileaks, Anonymous, government and military agencies and whistleblowers such as Edward Snowden.

On its own, Tor is not 100% all you need to secure yourself from surveillance, however.



Getting HTTPS Everywhere browser extension or the TOR browser bundle is the best option (as it includes HTTPS everywhere), which ensures encryption throughout. Tor is all well and good but on it's own it is vulnerable to a degree. Even if using Tor, Hackers could potentially still steal your information at the exit node, which is where the request reaches it's url. With HTTPS, this problem is dealt with. The data packets which send requests are now encrypted, as opposed to being simply darted through various IP locations.



I personally have used Tor with little problems in the past, and heard of hackers using it for various means and finding little security compromises. But, no harm in learning all this and applying it. There's a lot of shit going around about Tor, but it's mainly shilling, disinformation because the fact is, the dumb fucks at the NSA can't own it. So they resort to dirty tactics.

When it comes to VPNs and proxies, some people get the two mixed up. The two are very different concepts:

Proxy

Proxies are similar to VPNs but do not encrypt traffic. They are less secure but work great for basic browsing. Notably, they are also more often free or cheap, as opposed to VPNs (which usually cost money). Foxy Proxy is a common, usually reliable proxy. Keep in mind that both VPNs and proxies will slow down your traffic, since the data has to travel much further than normal. Cheap/free proxies are a horrible idea https://blog.haschek.at/post/fd9bc

VPN

A VPN (Virtual Private Network) is an end-to-end encrypted tunnel. So that's handy. Private Internet Access and TorGuard are good VPNs which do not keep user records (helping to protect you from government requests). VPNs work great for masking your location as well, helping you to take advantage of things like your Netflix subscription, even when you're traveling overseas. Anyone can set-up a VPN for free. For Linux a PPTP protocol is a simple, good choice **http://en.wikipedia.org/wiki/Virtual_private_network**

MAC Addresses

One aspect often overlooked when it comes to computer security is MAC addresses.

Each network interface on your computer or any other networked device has a unique MAC address. These MAC addresses are assigned in the factory, but you can change, or “spoof,” MAC addresses in software.

MAC stands for “media access control.” MAC addresses are also commonly referred to as physical addresses or hardware addresses, because they correspond to a hardware adapter.

Mac addresses are used for:

- **Static IP Assignment**: Routers allow you to assign static IP addresses to your computers. When a device connects, it always receives a specific IP address if it has a matching MAC address
- **Device Identification**: Many airport Wi-Fi networks and other public Wi-Fi networks use a device’s MAC address to identify it. For example, an airport Wi-Fi network might offer a free 30 minutes and then ban your MAC address from receiving more Wi-Fi. Change your MAC address and you could get more Wi-Fi. (Free, limited Wi-Fi may also be tracked using browser cookies or an account system.)
- **Device Tracking**: Because they’re unique, MAC addresses can be used to track you. When you walk around, your smartphone scans for nearby Wi-Fi networks and broadcasts it’s MAC address. A company named Renew London used trash bins in the city of London to track people’s movements around the city based on their MAC addresses. Apple’s iOS 8 will use a random MAC address each time it scans for nearby Wi-Fi networks to prevent this sort of tracking.

Bear in mind that each network interface has its own MAC address. So, on a typical laptop with both Wi-Fi and a wired Ethernet port, the wireless and wired network interface each have unique, separate MAC addresses.

Change MAC address on Windows

Most network cards will allow you to set a custom MAC address from their configuration panes in the Device Manager, although some network drivers may not support this feature.

First, open the Device Manager. On Windows 8.1, press Windows Key + X and click Device Manager. On Windows 7, press the Windows key, type “Device Manager” to search for it, and click Device Manager.

Locate the network interface you want to modify under Network Adapters, right-click it, and select Properties.

Click the Advanced tab and select Network Address in the list. Your network driver doesn’t support this feature if the option isn’t here.

Enable the Value option and enter your desired MAC address without any separating characters — don’t use dashes or colons. Click OK afterward.

Linux

Modern Linux distributions like Ubuntu typically use Network Manager, which provides a graphical way to spoof a MAC address.

For example, on Ubuntu you’d click the network icon on the top panel, click Edit Connections, select the network connection you want to modify, and click Edit. On the Ethernet tab, you’d enter a new MAC address under “Cloned MAC address” and save your changes.

Mac OS X

Mac OS X's System Preferences pane displays each network interface's MAC address, but doesn't allow you to change it. You can do so with a single command.

Open a Terminal window (press Command + Space, type Terminal, and press Enter.) Run the following command, replacing en0 with the network interface's name and filling in your own MAC address.

The network interface will generally be either en0 or en1, depending on whether you want to configure a Mac's Wi-Fi or Ethernet interface. Run the **ifconfig** command to see a list of interfaces if you're not sure of the appropriate network interface's name.

As on Linux, this change is temporary and will be reset when you next reboot. You'll need to use a script that automatically runs this command on boot if you'd like to permanently change your Mac address.

You can verify your change took effect by running a command that shows your network connection details and checking what MAC address your network interface reports afterwards. On Windows, run the **ipconfig /all** command in a Command Prompt window. On Linux or Mac OS X, run the **ifconfig** command.

If you need to change the MAC address on your router, you'll find this option in your router's web interface.

The standard format for printing MAC addresses in human-friendly form is **six** groups of two hexadecimal digits, separated by hyphens (-) or colons (:), in transmission order (e.g. 01-23-45-67-89-ab or 01:23:45:67:89:ab).

DNS Leaks- What are they?

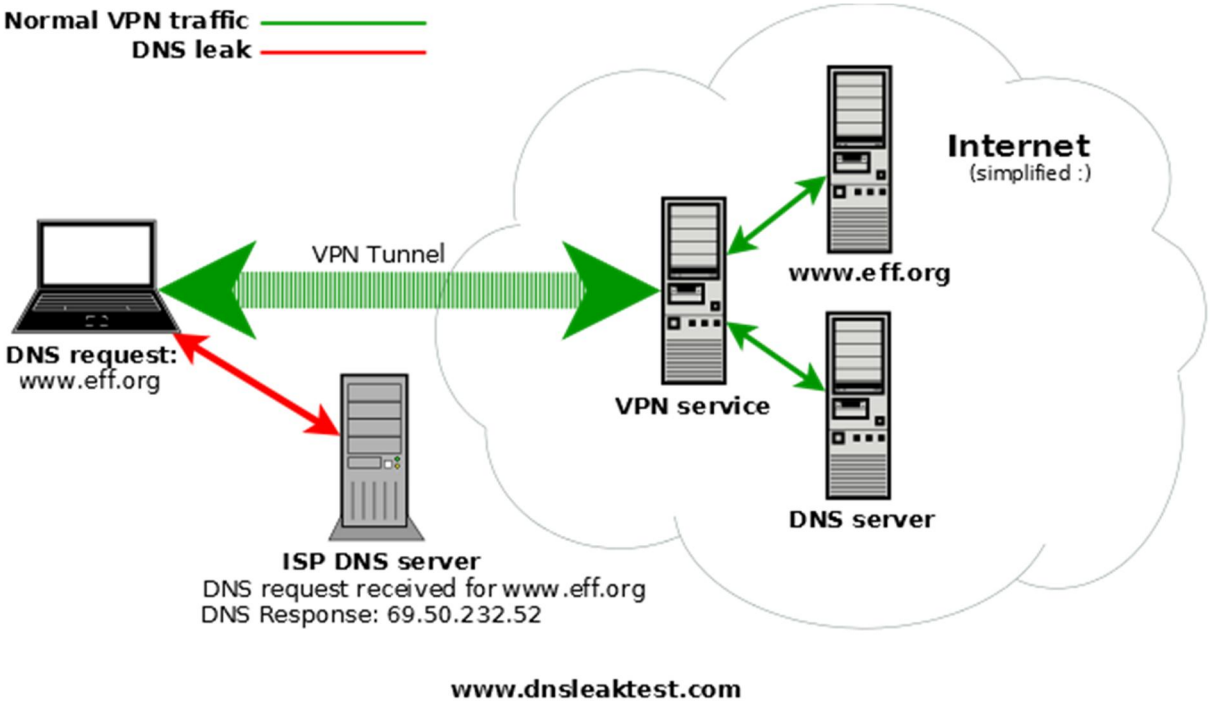
When using an anonymity service, it is important that all the traffic originating from your computer is routed through the anonymity network. If any traffic leaks outside the secure connection, anyone monitoring your traffic will be able to log your activity.

DNS or the Domain Name System is used to translate domain names such as national-action.info into numerical addresses e.g. 123.123.123.0 which are required to route packets of data on the internet.

Whenever your computer needs to contact a server on the net, such as when you enter a URL into your browser, your computer contacts a DNS serve and requests the IP address. Most Internet service providers assign their customers a DNS server which they control and use for logging and recording your Internet activities.

Under certain conditions, even when connected to the anonymity network, the operating system will continue to use its default DNS servers instead of the anonymous DNS servers assigned to your computer by the anonymity network.

DNS leaks are a major privacy threat since the anonymity network may be providing a false sense of security while private data is leaking.



To check for DNS leaks when using Tor or other VPNs go to dnsleaktest.com and run either the standard or extended test. The results displayed will detail how secure your connection is. It is also useful if you think someone is monitoring your traffic (through spyware etc).

Running a leak test on Tor etc will take quite some time, given how much your traffic is routed around. However, http://torguard.net/vpn-dns-leak-test.php lays out it simply. It is safe to say Tor Browser and TorGuard VPN are often secure against such DNS leaks.

Tor VPN can be purchased here: http://torguard.net/anonymoustorrentvpn.php

Some Key Points Regarding Tor

Don't torrent over Tor

Torrent file-sharing applications have been observed to ignore proxy settings and make direct connections even when they are told to use Tor. Even if your torrent application connects only through Tor, you will often send out your real IP address in the tracker GET request, because that's how torrents work. Not only do you deanonymize your torrent traffic and your other simultaneous Tor web traffic this way, you also slow down the entire Tor network for everyone else (noteworthy during times when multiple dissidents will be using it).

Don't enable or install browser plugins

The Tor Browser will block browser plugins such as Flash, RealPlayer, Quicktime, and others: they can be manipulated into revealing your IP address. Similarly, we do not recommend installing additional addons or plugins into the Tor Browser, as these may bypass Tor or otherwise harm your anonymity and privacy. The lack of plugins means that Youtube videos are blocked by default, but Youtube does provide an experimental opt-in feature that works for some videos.

Use HTTPS versions of websites

Tor will encrypt your traffic to and within the Tor network, but the encryption of your traffic to the final destination website depends upon on that website. To help ensure private encryption to websites, the Tor Browser Bundle includes HTTPS Everywhere to force the use of HTTPS encryption with major websites that support it.That "s" means that the website traffic is encrypted with the SSL protocol, making the traffic more secure. However, you should still watch the browser URL bar to ensure that websites you provide sensitive information to display a blue or green URL bar button, include https:// in the URL, and display the proper expected name for the website. Also see EFF's interactive page explaining how Tor and HTTPS relate.

Don't open documents downloaded through Tor while online

The Tor Browser will warn you before automatically opening documents that

are handled by external applications. DO NOT IGNORE THIS WARNING. You should be very careful when downloading documents via Tor (especially DOC and PDF files) as these documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP address. If you must work with DOC and/or PDF files, I strongly recommend either using a disconnected computer, downloading the free VirtualBox and using it with a virtual machine image with networking disabled, or using Tails. Under no circumstances is it safe to use BitTorrent and Tor together, however.

Use bridges and/or find company

Tor tries to prevent attackers from learning what destination websites you connect to. However, by default, it does not prevent somebody watching your Internet traffic from learning that you're using Tor. If this matters to you, you can reduce this risk by configuring Tor to use a Tor bridge relay rather than connecting directly to the public Tor network. Ultimately the best protection is a social approach: the more Tor users there are near you and the more diverse their interests, the less dangerous it will be that you are one of them.

There’s also a Tor app for Android mobile, known as Orbot.

Better than Tor- Tails

Tails is a ‘Live’ operating system which is built from the Linux OS (as opposed to Mac or Windows)

You can start it on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity, and helps you to:

- use the Internet anonymously and circumvent censorship;
  all connections to the Internet are forced to go through the Tor network;
- leave no trace on the computer you are using unless you ask it explicitly;
- use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging.

Tails comes with several built-in applications pre-configured with security in mind: web browser, instant messaging client, email client, office suite, image and sound editor, etc.

Tails is the equivalent of buying a computer and then throwing it away every time you use the internet. So it’s pretty secure.

Don't use Google

Google are sneaky little Jews, and keep records of everything to make more money and to appeal to their overlords.

When you search something in Google, it usually sends search terms to that site and your browser data and computer info. These sites thus build up a profile of you, and will bombard you with ads. Your online profile can also be sold.

Google, being a tool of the paranoid and power obsessed System, also saves all search histories of users. These search histories can be legally requested.

"Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to hand over user data. In this report, we disclose the number of requests we receive from each government in six-month periods with certain limitations. Usage of our services have increased every year, and so have the user data request numbers.

We continue to look for new ways to organize information and provide more detail. For example, starting with the July-December 2010 reporting period, we began to disclose the percentages of user data requests we comply with in whole or in part. And starting with the January–June 2011 reporting period, we began to disclose the number of users or accounts about which data was requested.

Our FAQ about legal process provides information about how we aim to put users first when we receive user data requests. To learn more about the laws governing our disclosure of user data and reforms to those laws that we think are important, visit http://digitaldueprocess.org/. We hope this report will shine some light on

the appropriate scope and authority of government requests to obtain user data around the globe." -Google

Delete tracking data regularly: Your browser keeps track of where you go, what you type, and any other data it can capture about you. A basic security measure is to regularly delete this data (history, cookies and cache).

Download CCleaner: This scrubs your hard drive, internet search history, cache and cookies squeaky clean, as well as containing other features. Highly recommended and 100% free: https://www.piriform.com/ccleaner/download (you can buy the Premium version for around $30, and it's pretty based).

Use Linux: Micro$oft are one of THE greediest, do gooder corporations out there, and should be avoided and boycotted at all cost (I purchase nothing from them, and will avoid any phone which uses their software or operating system). Windows is also notoriously unsafe, given most viruses are designed to infect Windows operating systems, as these make up the majority of personal computers. Microsoft provide an entry key for the police which bypasses all Windows password encryption.

Linux is generally considered to be one of the most secure operating systems but it has a slight learning curve. But it soon becomes second nature, and is probably the best thing you will do when it comes to securing online privacy and computer protection. Ubuntu is the best place to begin.

Take precautions with your email: Use secure email services when you can. Use a dummy email address when emailing people you do not trust and make sure that that dummy email is not attached to any of your real information (use a fake name, age, etc). You can also set up emails to reroute, so that you can receive them at your normal address. Just make sure that you reply from the dummy account! This is not particularly secure against government agencies but it is fairly secure against hackers. However, there are disposable, temporary emails you can set up and use which are then deleted after a while, such as Guerilla Mail.

When it comes to making dummy accounts, a great site is http://www.fakenamegenerator.com.This site creates a wealth of fake information, from name and address, to email and eye colour. It even generates social security numbers and other realistic criteria.

Proton Mail is an up and coming anonymous email provider which was developed by researchers at CERN. It uses state of the art cryptography and a cast iron promise that employees are unable to access your data. Given Swiss laws, it is also notoriously difficult for agencies to request information from companies, nigh on impossible.- https://protonmail.ch/

It is recommended that Protonmail is used by any and all serious Nationalists.

Use Bitcoin: Bitcoin is a largely untraceable form of currency which has gained a lot of attention in the last year or two. Not every website accepts it, but for the websites that do, this can be a great way to help protect your identity when making purchases.

Use secure passwords which use at least 8 characters, uppercase letters, lowercase letters, numbers, and characters. Never use dictionary words in your password, either. Do use different passwords for every site you have an account with, if possible. Change your passwords frequently (monthly is what I do). And don't write all your passwords down in a jotter, for someone to find. Some security sites have password safes, which come in handy.

For creating good, strong passwords, check out **www.identitysafe.norton.com/password-generator**

Don't go to untrustworthy sites or click on emails from unknown addresses. Be wary of porn sites. These are notoriously infected. Also file sharing sites.

Get a hard drive encryptor: These are pretty useful gadgets when they're not being made by Window$. Truecrypt used to do the trick, but it was abandoned by the author and is untrusted in many circles. However, the project has been taken up by developers and s back and running, from what I've seen. There was an audit of version 7.1a and it was seen to be pretty ok. This is thanks to open source, which allows transparent reading of source code and further development. Practically every Jewish owned information company has been explicitly anti-open source, which is interesting. A search for hard drive encryptors should yield a good set of alternatives.

Social Media: Facebook, being the ZOG tool that it is, is growing less and less fond of user privacy. However, there are steps you can take, and it all depends primarily on how much info you put on there about yourself. So think about that.

Using A Virtual Box

Whilst Linux might prove a challenge for some, it's security credentials cannot be underestimated. Given that most viruses and spyware are built for Windows systems, having a Linux computer makes intrusion much more difficult. Linux is also free from the myriad of backdoors Windows creates for the authorities. I could go on all day about the pros of using Linux.

One excellent way of getting the security boost of Linux and easing the learning curve is by running a Windows Virtual Box, also referred to as a Virtual Machine within a Linux system (you can do the opposite too- run a Linux VB in your Windows computer to get used to using it without installing Linux straight away).

Virtual Machines have been used in this way by hackers and cyber security activists with great success.

Step 1- Download Virtual Box

https://www.virtualbox.org/wiki/Downloads

Step 2- Learn how to run it

https://www.virtualbox.org/manual/UserManual.html

Appendix I-

Anti Forensics

Anti-computer forensics (sometimes counter forensics) is a general term for a set of techniques used as countermeasures to forensic analysis.

Anti-Forensics is the art of leaving no trace on your computer. It is combating common forensic tools in preventing any penetration for forensic tests on your computer. It can pretty much be summed up with one famous quote "Make it hard for them to find you, and impossible for them to prove they've found you."

Because Linux installations are pretty much already secured, this guide will only focus on Windows. Windows is a security nightmare, and I would strongly advise getting to grips with, and downloading, a Linux OS. VPNs, proxies, and Tor only get you so far, but what do you do when they've traced it to your computer?

This guide is designed to help you prevent them from proving you've done anything wrong even if they have your computer.

Disabling Time Stamps

Using Time Stamps, forensic experts can build a 'digital time-line', this can be very compelling evidence when cross-referenced with other known evidence. In order to strengthen security, we must disable these logs.

Step 1- User Assist File

There is a registry setting that keeps logs and dates of all launch programs, forensic experts can use this to build a digital timeline, we must disable this for computer security. Navigate to HKEY_Current_User\Software\Microsoft\Windows\Currentversion\Explorer\User assist. (Do this by hitting the Windows button on your keyboard and R at the same time and typing regedit in For Windows 8, this guide is invalid. Answer? Don't use Windows 8- or do some research yourself).

You should see two subkeys called Count, delete both these keys. Now right-click the UserAssist key and create a new key named 'Settings'. In this key (right clicking on it) create DWORD value named NoLog, set the value to 1.
Windows will no longer store hidden logs of the exact times you have been accesing files, therefore forensics experts can no longer use these hidden logs to create a digital timeline.

Step 2 - Last Access Logs

Next we will disable the last access in Windows. What last access is is a setting on Windows that allows you to see when you opened, modified, and/or created files on your computer and is similar to the UserAssist registry key. By disabling this forensic experts won't as easily be able to tell when you've been accessing programs or files on your computer.

To disable last access open command prompt on your computer, if on Vista or Windows 7 make sure to run as administrator. In command prompt type the following: fsutil behavior set disablelastaccess 1

Last access has now been disabled, in order for it to take effect you must restart your computer. (You have to have admin rights to do this).

Appendix II
Encrypting Your Computer

It is very important to make sure that your computer is encrypted, in the case an unwanted visitor is trying to access your computer, they will not be able to access to computer if it is encrypted.

Step 1 - Open-Source Disk Encryption

To encrypt your computer, you can use hard drive encryptors. This is also very secure, but you may be forced to give up your password due to court-order (In this situation, if you are a VERY good liar, you could simply say 'I forgot', but you would have to make it believable- according to time frames, this can work. If say, you are arrested and bailed and the police do not come to you for a month or more, then turn up demanding the password, you can simply say your forgot- and inwardly relish at their frustration).

TrueCrypt 7.1a

A good tool to use for encryption is TrueCrypt. Whilst the developers abandoned the project, TrueCrypt is opensource, meaning future generations can develop and implement it further. TrueCrypt devs now recommend BitLocker as an alternative, but Bitlocker is a Microsoft creation, and will no doubt have backdoors for police investigators.

The latest iteration of TrueCrypt, which stands up to security tests is 7.1a.

Download it and if you are having trouble, here's a simple tutorial. Further research should allow you to understand how to use this program in more depth.

Step 2 - Encrypt Your Keystrokes

You need to protect yourself from keyloggers. As strange as it may sound even the government has keyloggers, a few years ago the law speculation about CIPAV, a government spyware known to send the users IP address, Mac address, open ports, operating system, installed applications, default web browser, visited URLs, logged in user, etc...

In order to protect yourself from keyloggers, you should encrypt your keystrokes. You can do this using a software called 'Keyscrambler'. Please note, you should NOT use the free version of Keyscrambler, you should only use the Premium version, which costs a decent sum of money. Or get it off a torrent site i.e kat.ph, thepiratebay.se etc.
[*Link supplied upon request- just email me*]

Keyscrambler Premium supports 170 programs, including windows logon, most web browsers, and popular IM programs (i.e. Skype).

Keyscrambler Personal works as a browser extension for Firefox and IE.

Making Encryption Secure

Encryption is pointless if it can be easily bypassed or overcome. You need to make sure that the encryption is secure too.

Step 1 - Make Sure Your Password Is Strong

Even with your computer encrypted, it is still vulnerable. Make sure your password is good (for optimal security, your password should be twenty or more characters, with symbols, numbers, and random capitals, and a special symbol (like ALT+1456) really increase security). Norton password generator is great for this.

Step 2 - Get A Good Anti-Virus

This may seem obvious, but all this is pointless if you get infected with a keylogger that takes screen shots. Having a good anti-virus is one of the most important things you can do. You should consider McAfee, BitDefender, ESET, Nod32 and Kaspersky. Advance System Care Ultimate is good too.
In theory, you rarely even need anti-virus software when using Linux, as most viruses are built to infect Windows systems, given these make up the majority of computers, but it's best to be safe. Especially if using a Linux tailored to end users, such as Ubuntu or Mint.

All anti-virus programs are expensive, but for the other anti-virus you can torrent them from i.e Kat.ph, ThePirateBay.se, or one of your choice. Just make sure you find one with a lot of seeders and read the comments. Also Malwarebytes Pro is a must.

Disabling Windows Hibernation

You may as well hand your computer over to the feds if they raid your house and your computer is in hibernation. Also, putting your computer into hibernation is pretty much just taking a screen shot of your RAM that gets saved to your hard drive.

To disable hibernation in Windows Vista/7:
Open your Control Panel. Click System and Security, then click 'Power Options'.
Click 'Change plan settings' for you current power plan.
Now click 'Change advanced power settings'. Expand 'Sleep', then expand 'Hibernate
After'. Enter “0" for 'Setting:' to set hibernate to 'Never'.
Hibernation is now disabled.

Disable and Remove USB Logs

Next on the list of Anti-Forensics in to disable logs of USB activity, flash drives, etc...

This can be valuable if you have a flash drive with sensitive data and you don't want any logs of it ever being plugged it to your computer.

Step 1 - Delete the USBSTOR Registry Setting

The USBSTOR setting contains history of plugged in USB devices.
To delete it, hit the WINDOWS Home Button + R at the same time. This will open up 'Run'; type: "Regedit" (without quotes). Browse to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
Now, right click 'USBSTOR' and hit 'Delete', then confirm that you want to delete the key. Now, the key has been deleted.

Step 2 - Delete The Setupapi.log File

The Setuppapi.log is a plain-text file that stores the list of installed USB devices and their drivers. We will delete it with a program called CCleaner.
CCleaner is actually one of the best anti-forensic tools out there, and its free.
Download for free from this site; https://www.piriform.com/ccleaner/download

Windows Security Misc

This is for the shit that has to do with windows anti-forensic security, but wasn't big enough to have its own section. That does NOT mean this section isn't important, the stuff in here may actually be the most important in the whole guide.

Step 1 - Disable System Restore Points

System Restore points can be used to bring your computer back to a date when it wasn't secure and can also be used to restore
overwritten files.
To disable System Restore points, right click 'Computer' and click 'Properties'.
Now click 'Advanced System Settings'. Under 'System Protection' click 'Configure'.
Now, select 'Turn Of System Protection' and apply it.

Step 2 - Disable 'Send Error Report to Microsoft

This is self-explanatory, we obviously don't want Microsoft having logs of all

our crashed programs. To do this, go to your start menu and search 'problem reporting settings' and then click on 'Choose How To Report Problems'. Click 'Change Report Settings For All Users' and then set it to 'Never check for solutions'.

Step 3 - Wipe With CCleaner

This is the heart of Anti-Forensics right here. CCleaner is actually one of the most powerful Anti-Forensic tools, -IF- used correctly.

As it turns out, when deleting files, you DO NOT need to do multiple overwrites. With modern hard-drives, one overwrite really is enough to delete a file beyond repair, even though it is popular belief that you need several overwrites to be secure.

With CCleaner, I would recommend three overwrites, just in-case it misses something the first time around (remember, it is a free software).

Once you have CCleaner installed, run it (AS ADMIN), go to 'Settings' and make sure you have it set to overwrite deleted data with three passes. Go back to 'Cleaner' and check EVERYTHING. I mean EVERYTHING, and hit 'Run Cleaner'. You might want to leave this on overnight.

Do this everytime you are done with a major hacking job. When using normally (what should be every time you are done with your computer), uncheck 'Wipe Free Space', this will cut down the time from hours to a few minutes.

Step 4 - Disable Debugging Upon Failure

This keeps logs of your computers failures and blue screen info.
To disable it, right click 'Computer' and go to 'Advanced System Settings', now go to 'Start Up and Recovery'. Now, set 'Debugging Information' to 'None'.

Step 5 - Disable Windows Event Logging

Windows keeps logs of all events on the computer. First, before we disable, we must clear all the logs.

To disable it, go to Control Panel then System and Security. Now, click Administrative Tools, and then Event Viewer. In either pane of the Event Viewer window, right-click System and then select Clear All Events, you will get a window that says: "Do you want to save 'System' before clearing it?", click 'No'.
Now we must disable Windows Event Logging. Go to 'Run' and type in 'msconfig', then go to 'Services' and make sure 'Hide all Microsoft Services' is UNCHECKED. Now scroll down until you find 'Windows Event Logging', and UNCHECK it.

Now restart your computer right away.

Preventing being found in the first place

You should never be tracked in the first place. Follow these guide lines to stay anonymous:

- Use Tor or Tails for web browsing you wouldn't want the Police, or your ISP looking at.

- Never release personal information online and use different aliases. Never connect ANY real information to your hacking alias. Build fake information if you are paranoid. fakenamegenerator.com might help with this.

- Don't get lazy, and be patient.

Summary

- *Use Tor*

- *Get AntiVirus*

- *Try using Linux*

- *Use Truecrypt*

- *Use Keyscrambler*
- *Use Protonmail*
- *Use CCleaner*
- *Get a Tails stick*
- *Do your homework*

Appendix III- Useful Resources

I hope you do your research and continue to learn everything about keeping safe. Here's a few links which you will find useful.

https://www.eff.org/- Electronic Frontier Foundation site

https://www.us-cert.gov/ncas/tips -United States Computer Emergency Readiness Team

http://iag.me/tech/10-tips-to-make-your-computer-more-secure/- 10 Handy Tips

http://en.wikipedia.org/wiki/Computer_security- Good Wiki article

https://www.sans.org/tip_of_the_day.php -Security Awareness Tips

https://ssd.eff.org/en/playlist/activist-or-protester- A guide for activists and protesters created by the Electronic Frontier Foundation.

https://ssd.eff.org/en/playlist/online-security-veteran#introduction-public-key-cryptography-and-pgp- An EFF guide to PGP

https://techtoolsforactivism.org/- Site containing a wealth of resources. Very useful.The list of software and media is especially helpful.

http://www.gimp.org/downloads/- Gimp Image software. Just as good as Photoshop, and free.

https://fakeinbox.com- No prizes for guessing what this is.

https://privnote.com- Self-destructing temporary notes.

https://disconnect.me- Browser add-on for filtering and preventing online tracking.

https://identitysafe.norton.com/password-generator- Random password generator (gives tips on creating strong passwords)

http://www.fakenamegenerator.com/- Generate an entire fake id. Excellent for fake forms etc.

http://www.datafakegenerator.com/- Generate not only name, address etc. but credit card details too.

http://www.whatsmyip.org/- Self-explantory. Tor usually covers this problem, but always safe to double check and see what your ip is. The site also contains great tools you'll learn about in time, including DNS leaks and stuff.

https://www.torproject.org/projects/torbrowser.html.en - -Excellent VPN, contains built in: browser,proxy routed, https everywhere, tons of privacy features. Saves a lot of time.

After you install Tor, you can enter 'the deepweb' aka the darknet. Here is a list of deepweb addresses: http://deepweblinks.org/

-RM

2015